Обратный остаток

Обратное по модулю целого a — это такое целое число x, что произведение ax сравнимо с 1 по модулю m.

Теорема. Если $(a, m) = 1$, то у a есть обратный остаток по модулю m.

$\boxed{1}$ Дано простое число p и его некоторый ненулевой остаток a.

(a) Докажите, что в последовательности $0 \cdot a, 1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a$ все числа дают разные остатки по модулю p.

(b) Докажите, что существует и при том единственный обратный остаток b

(c) Какие остатки совпадают со своими обратными остатками?

$\boxed{2}$ Решите сравнения (то есть найдите все подходящие x и докажите, что других нет)

(a) $5x \equiv 2 \pmod 3$;

(b) $3x \equiv 2 \pmod{11}$;

(c) $6x \equiv 1 \pmod{13}$;

$\boxed{3}$ Какой остаток даёт x при делении 13, если:

(a) $3x \equiv 4 + x \pmod{13}$;

(b) $7x \equiv 8 + 3x \pmod{13}$;

(c) $10x + 2 \equiv -x \pmod{13}$.

$\boxed{4}$ **(Теорема Вильсона.)** Докажите, что $(p-1)! \equiv -1 \pmod p$, если и только если p является простым числом.

$\boxed{5}$ Пусть p – простое число и $k \leqslant p$. Докажите, что $(p-k)!(k-1)! \underset{p}{\equiv} (-1)^k$.

$\boxed{6}$ Для простого числа p и остатка a определим его *показатель* по модулю p как наименьшее такое натуральное число d, что $a^d \equiv 1 \bmod p$. Рассмотрим произведение всех остатков по модулю p, которые имеют одинаковый показатель. Какой остаток от деления на p даёт это произведение?

$\boxed{7}$ Пусть числа p и $p+2$ являются простыми числами-близнецами. Докажите, что справедливо $4((p-1)!+1)+p \equiv 0 \pmod{p^2+2p}$.

$\boxed{8}$ Даны натуральные числа a, b и c такие, что $ab + 9b + 81$ и $bc + 9c + 81$ делятся на 101. Докажите, что тогда и $ca + 9a + 81$ тоже делится на 101.

$\boxed{9}$ Пусть $p \geqslant 3$ — простое число. Докажите, что если сумму $\frac{1}{1} + \frac{1}{2} + \ldots + \frac{1}{p-1}$ привести к общему знаменателю, то числитель получившейся дроби будет делиться на p.

$\boxed{10}$ На доске написаны числа $\frac{100}{1}, \frac{99}{2}, \ldots, \frac{1}{100}$. Можно ли выбрать какие-то девять из них, произведение которых равняется единице?

$\boxed{11}$ Докажите, что для любого простого $p > 3$ существует бесконечно много n таких, что $2^n + 3^n + 6^n - 1$ делится на p.